Statement of the Honorable Greg Walden
Chairman, Subcommittee on Communications and Technology
Hearing on "Cybersecurity: Threats to Communications Networks and Private-Sector Responses"
February 8, 2012

Back in October, the *House Republican Cybersecurity Task Force* recommended that the committees of jurisdiction review cybersecurity issues. This hearing continues our committee's review of cybersecurity issues with an examination of threats to communications networks and the responses of the private sector.

Threats to communications networks have come a long way in a short time. Before coming to Congress, I spent 22 years as a radio broadcaster. As a small businessman, I had to worry about securing our communications network, and back then it was relatively straightforward. Maybe you bought a fence to surround your broadcast tower. Maybe you hired a security guard to watch your station at night. But physical security was the concern.

Not anymore. While physical security remains important, cybersecurity has also become a pressing concern. Now a small business confronts a dizzying array of threats online from the Zeus trojan horse to Stuxnet from lulzsec to botnets. These threats are serious. Unless our cyberdefenses hold, a bad actor could drain the bank account of a business, crash an online company's website, or launch a barrage of cyberattacks on a company's network. Those are serious consequences for any business, and especially for the small businesses that are at the heart of creating new jobs in our economy.

Every month, we learn more about these cyberthreats. And what we have learned thus far worries me. I am worried that our communications networks are under siege. I am worried that the devices consumers use to access those networks are vulnerable. I am worried that our process for looking at communications supply chain issues lacks coordination. And I am worried that our cyberdefenses are not keeping pace with the cyberthreats.

In this hearing, we are lucky to have the voices of five private-sector witnesses to guide us through the complex issue of cybersecurity. I am hoping that you will tell me that cyberspace is secure. Unfortunately, I expect that you will tell us that the threats to our communications networks are all too real and that American businesses are losing dollars and jobs because of cybercrime and cyberespionage, and that our national security is potentially at risk, as well.

I also expect that you will explain what the private sector is doing to fortify our cyberdefenses. The private sector owns most of the critical infrastructure—the wires, the servers, the towers and base stations—that make up our communications networks, and they are on the front lines of cybersecurity. I want to know what cybersecurity services are being offered to consumers, what protections are being deployed in our communications networks, and what affirmative steps the private sector has taken to lock down the supply chain and to combat cybercrime.

I also expect to hear what you think the appropriate role of the federal government is. Are federal laws and regulations helping or interfering with information sharing? Are federal regulations of cybersecurity practices appropriate? Should the federal government be providing incentives for Internet service providers and other members of the private sector to invest and innovate in the cybersecurity arena? And how should our country's fiscal state shape our discussion of the federal role?

These questions and others will form the basis for deciding what cybersecurity legislation, if any, is needed in the near term, and how we can best secure cyberspace in the long run. I thank the panelists for their testimony today, and I look forward to a lively discussion of these issues.